MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2016/2017

ETM7106 – NETWORK SECURITY

15 OCTOBER 2016
9:00 A.M. - 12:00 P.M.
(3 Hours)

INSTRUCTION TO STUDENT

1. This examination paper consists of 8 pages including cover page with 4 Questions only.

2. Attempt **ALL** the questions. Each question carry equal marks and distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided. Please number your answers clearly.

Question 1

a) A small organisation has 20 members. How many secret keys are needed in each of the following settings if a symmetric encryption is used?

i) All members of the organisation need to send secret messages to each other.

[2 marks]

ii) Everyone trusts the president of the organisation. If a member needs to send a message to another member, s/he first sends it to the president; the president then sends the message to the other member.

[1 mark]

b) Carol can use only the additive cipher on her computer to send a message to a friend. She thinks that the message is more secure if she encrypts the message three times, each time with a different key. Show that this does not improve the security of the cipher.

[4 marks]

c) We know that public key cryptosystems can provide non-repudiation of origin. Now consider a secret key cryptosystem, in which Alice and Bob share a secret key. Bob has a message that he claims came from Alice, and to prove it he shows both the plaintext message and the ciphertext message. The ciphertext corresponds to the plaintext enciphered under the secret key that Alice and Bob share. Please explain why this does not satisfy the requirement of non-repudiation of origin?

[4 marks]

d) Explain THREE general ways that entity authentication can be performed by users to log on to a network remotely. Why some organizations implement multifactor authentication for their network system?

[4 marks]

e) Your friend has received an e-mail as shown in Figure Q1.1. She needs your advice on whether she should reply the e-mail and click the link as requested. Justify your answer and suggest some of the actions that she should take.

[4 marks]

Subject: Confirm Your MMU University Webmail Account in Order To Avoid Closure
From: "MMU University"
Date: Wed, 20 July 2016 11:33:02 +0300 (EAT)
To: undisclosed-recipients:;

Suspicious access to your account detected, It would appear that another person has been accessing your e-mail account recently.
If you do not want to lose access to your account, please click here and follow the instructions for verification.

Continued...

Figure Q1.1

f) You have implemented a password authentication system that requires user to choose a password which comprises six upper case letters (A~Z).

i) Calculate the number of possible passwords.

[1 mark]

ii) An attacker has obtained a copy of an encrypted password file. He uses an automated program with an encryption rate of 5 million encryptions per second. How long will it take to test exhaustively all possible passwords?

[2 marks]

iii) You plan to improve the security of the system by increasing the length of the password requirement to 10 characters long and comprising of uppercase (A~Z) and lowercase (a~z) letters, and numeric digits (0 ~ 9). If the same automated program is used, how long will it take to test exhaustively all possible passwords?

[3 marks]

Continued...

Question 2

a) The round function of the *Advance Encryption Standard (AES)* block cipher consists of 4 sub-functions, namely SubBytes, ShiftRows, MixColumns and AddRoundKey. For the last iteration, there is no MixColumns operation. Given that a 10-round AES with the 128-bit subkey for the last iteration is "**FF 89 85 C5 8C FA AB 96 73 4B 74 83 13 92 0E 57**" and the State after the 9th iteration is as follows:

D8	**E4**	**49**	**5F**
F7	**29**	**8C**	**2C**
60	**39**	**75**	**F1**
62	**9E**	**D0**	**F6**

i) Show the values of State after *SubBytes* (The AES S-Box is shown in Figure Q2.1).

[2 marks]

ii) Show the values of State after *ShiftRows*.

[2 marks]

iii) Show the values of State after *AddRoundKey*.

[2 marks]

hex	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

x

The Substitution Table – Sbox[xy] (in hexadecimal)

Figure Q2.1

b) With the aid of a diagram, describe clearly the Electronic Codebook (ECB) mode of operation.

[4 marks]

c) Explain the main weakness of electronic codebook (ECB) mode of operation and how this problem can be overcome by using cipher-block chaining (CBC) mode.

[4 marks]

Continued...

d) Based on what are known to the attackers, list and explain any *TWO* types of cryptanalytic attacks.

[4 marks]

e) Alice generates the public key $(e, n) = (13, 33)$ to be used in an RSA cryptosystem. She uses this cryptosystem to encrypt a message "**710**" and sends to Bob.

i) Determine the private key of Alice using the *extended Euclidean algorithm*.

[4 marks]

ii) Use the *Square-and-Multiply algorithm* to demonstrate the encryption process and find the ciphertext.

[3 marks]

Continued...

Question 3

a) A wireless network system uses the following protocol to establish a session key. Device A generates a public and secret key pair (PK_A, SK_A). It sends PK_A and the IP address (IP_A) to device B. Device B generates the session key K_s and sends it to A encrypted using PK_A. A decrypts the session key with SK_A and they both use the session key K_s for subsequent communication. The following summarises the protocol messages between A and B, where || denotes concatenation; $E_{PK_A}(K_s)$ is encryption of K_s under public key PK_A.

$$A \rightarrow B : PK_A \,||\, IP_A$$
$$B \rightarrow A: E_{PK_A}(K_s)$$

Show how an attacker on device C can mount a *man-in-the-middle* attack.

[6 marks]

b) Your boss reads through an article on current security threat related to 'WarDriving'. Explain in detail on what and how this attack is possible.

[4 marks]

c) Anonymity is one of the major areas of mobile systems security. Anonymity is defined as the state of being not identifiable within a set of principles. Give FOUR of the issues that should be considered to solve the anonymity problem.

[4 marks]

d) Discuss TWO problems that can be encountered in the usability of Bluetooth device in any context.

[4 marks]

e) Attacks in the wireless communications environment are particularly troublesome because they are easy to execute yet impose significant overhead on user or the

wireless network. Describe *interception attacks* on wireless communications and discuss the remedies for the attacks.

[4 marks]

f) You are thinking to run an e-commerce using online transaction through web browser. Explain when using HTTP would be satisfactory and why, and when you and your clients should use HTTPS and why.

[3 marks]

Continued...

Question 4

a) As a new security engineer, you have been assigned to deploy a packet filtering firewall for a network as shown in Figure Q4.1. The network consists of a router, a firewall, a public Web server (IP address = 5.6.7.8), an external e-mail server (IP address = 5.6.7.9), and 5 internal workstations (IP address range: 192.168.1.2 – 192.168.1.6). The firewall consists of three interfaces, namely eth0, eth1, and eth2. The firewall rule syntax is defined as follows:

<allow/drop> <protocol> <ip_address>:<port> /<interface> → <ip_address>:<port> /<interface>

Example: **allow tcp *:* /eth0 → 1.1.1.1:25 /eth1**

Write the packet filtering ruleset for this firewall based on the following security policy:

- By default, block all inbound connections.
- Allow all inbound TCP connections to SMTP on the e-mail server (port 25).
- Allow all inbound TCP connections to HTTP on the Web server (port 80).
- Allow all outbound connections.

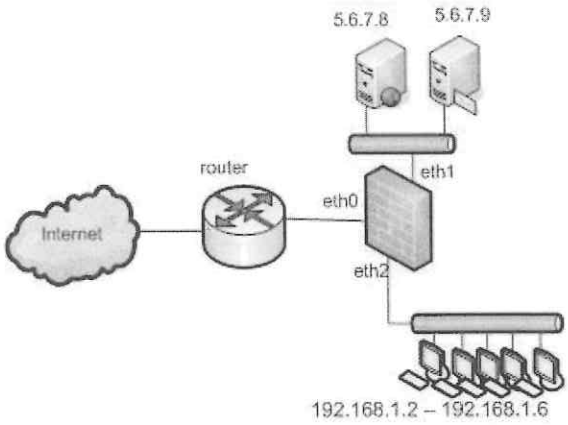

Figure Q4.1

[7 marks]

b) With the aid of a diagram, explain the anti-replay mechanism in IP Security (IPSec).
[5 marks]

Continued...

c) You realise that a new installed network-based intrusion detection system (IDS) has been generating a lot of alarms. Your manager wants to know how this will affect the company's network. Write a description to explain to her about the following concepts.

i) What are false positives and negatives?
[2 marks]

ii) Provide a suggestion to reduce the false alarms.
[1 mark]

iii) Discuss the advantages and disadvantages of network-based intrusion detection systems.
[4 marks]

d) Describe briefly the following activities in a vulnerability assessment. Give an example of a tool that is used in each assessment activity.

i) Reconnaissance

[3 marks]

ii) Network Service Discovery

[3 marks]

End of Paper